CASE STUDY

SecurityScorecard in the Critical Infrastructure Sector

Municipal-owned Utility Fortifies Supply Chain Security

Canadian power distributor enhances vendor risk management and regulatory compliance

The Challenge: Ineffective TPRM program

As a power distribution company operating critical infrastructure and handling sensitive customer data, the organization recognized opportunities to improve the efficiency and effectiveness of its third-party vendor risk management. Their reliance on manual, yearly questionnaires for a large vendor base proved time-consuming and difficult to track, occasionally leading to delays and gaps in visibility. Vendors sometimes provided high-level affirmations that were difficult to verify, limiting full visibility into the supply chain's security posture.

The organization also encountered external pushback, as vendors were reluctant to provide detailed information. Keeping pace with evolving frameworks such as NIST proved complex, highlighting the need for more streamlined and proactive approaches.

The regulatory environment shifted dramatically in 2025, moving from vendor self-attestations to external verification of security controls. This change, coupled with recent cyberattacks on other power distribution companies linked to third-party breaches, underscored the urgent need for a robust and verifiable supply chain security program. The organization determined that advancing beyond traditional methods was essential to effectively address evolving threats and meet new compliance expectations.

Key Benefits

- Enhanced cyber resilience
- Proactive risk mitigation
- Improved regulatory adherence

> **SecurityScorecard translates complex cybersecurity findings into actionable insights for our board and leadership, fostering informed risk governance.**
>
> Director of IT

Customer Info

Industry
Power Distribution

Headquarters
Canada

Products
Security Ratings,
Security Questionnaires

SecurityScorecard.com
info@securityscorecard.com

About the Customer

The organization is a power distribution company serving customers in Canada. It operates critical infrastructure and manages sensitive customer information, necessitating a strong cybersecurity posture across both internal systems and external partnerships. With a lean IT team, third-party risk and supply chain cybersecurity responsibilities are integrated into broader IT and security operations. This structure reinforces the need for efficient, scalable processes to evaluate and monitor the cybersecurity practices of technology partners, ensuring risks are managed consistently across the extended environment.

The Solution

The organization sought a comprehensive solution to automate and enhance their third-party risk management process, moving beyond their manual, questionnaire-based approach. After evaluating several options, they ultimately selected SecurityScorecard. The decision was driven by SecurityScorecard's robust threat intelligence and actionable insights, which support proactive risk management and help maintain vendor trust. The transparency of SecurityScorecard's scoring methodology enables the organization to effectively align with vendors on which issues should be prioritized for remediation.

> **The platform empowers us to rapidly identify and mitigate third-party risks and exposures, significantly enhancing our response capabilities and reducing potential impact.**
>
> Director of IT

Continuous Monitoring

SecurityScorecard's continuous monitoring capabilities allow the organization to gain real-time visibility into their supply chain's security posture. This means they can be immediately aware if a vendor's security deviates from agreed-upon standards, such as an unauthorized port opening, or if their name appears in hacker chatter.

Streamlined Questionnaires

The platform provides tools to automate and streamline the vendor questionnaire process. By using SecurityScorecard, the organization can ensure vendors complete assessments efficiently and that their responses are verified against objective security ratings, improving the accuracy and reliability of vendor risk data.

Intuitive Reporting

A key differentiator for the organization was SecurityScorecard's executive-ready dashboard and intuitive reporting. The visual representation of vendor security scores allows for informed discussions on risk acceptance and mitigation strategies, ensuring that cybersecurity is given the necessary attention at the executive level.

Why SecurityScorecard

The organization aimed to modernize its vendor assessment process by moving to an automated system that delivers more accurate and timely data. This will enable them to proactively identify and address vulnerabilities within their supply chain, reducing their overall risk exposure. Furthermore, the verifiable data and clear reporting from SecurityScorecard will help the organization demonstrate adherence to regulatory frameworks and build greater trust with their customers and stakeholders.

> **The platform empowers us to rapidly identify and mitigate third-party risks and exposures, significantly enhancing our response capabilities and reducing potential impact.**
>
> Director of IT

Enhanced cyber resilience

By leveraging objective security ratings, the organization can hold vendors accountable for their cybersecurity practices. This data supports more informed negotiations, drives stronger security commitments, and ensures vendors are meeting clearly defined expectations aligned with corporate cybersecurity standards.

Proactive risk mitigation

The continuous monitoring capabilities of SecurityScorecard will allow the organization to be immediately aware of any security incidents or vulnerabilities affecting their vendors. This enables them to take swift, proactive measures, such as temporarily shutting down access, to prevent potential breaches from impacting their own environment or customer data.

Improved regulatory adherence

As cybersecurity regulations evolve to require independent verification of security controls, SecurityScorecard's objective security ratings and continuous monitoring capabilities offer a clear and defensible position. The ability to present a dashboard and a structured process for vendor monitoring will demonstrate to regulators and customers alike that the organization is proactively managing third-party risk, ensuring compliance with cybersecurity standards and regulations